Thursday October 17

Recall from Tuesday:

Definition: If p is an odd prime, define the Legendre symbol $\left(\frac{a}{p}\right)$ as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue } (\text{mod } p), \\ -1, & \text{if } a \text{ is a quadratic nonresidue } (\text{mod } p), \\ 0, & \text{if } p \mid a. \end{cases}$$

Theorem: If p is an odd prime, then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

($p \mid a$ case is obvious, so assume $p \nmid a$)

Proof 1: Euler's criterion: $x^2 \equiv a \pmod{p}$ has $\begin{cases} 2 \text{ solutions}, & \text{if } a^{(p-1)/2} \equiv 1 \pmod{p}, \\ 0 \text{ solutions}, & \text{if } a^{(p-1)/2} \equiv -1 \pmod{p}. \end{cases}$ //

Proof 2: The product of all reduced residue classes (mod p) is $(p-1)! \equiv -1 \pmod{p}$ by Wilson's theorem. Let's pair these classes:

- For every $(b,p)=1$, there's a unique $(c,p)=1$ such that $bc \equiv a \pmod{p}$. (Indeed, $c \equiv b^{-1}a \pmod{p}$.) This is a true pairing ($b \equiv c^{-1}a \pmod{p}$).
- If b is paired with itself, then $b \cdot b \equiv a \pmod{p}$, as $b^2 \equiv a \pmod{p}$.

— If a is a quadratic nonresidue, then

$$-1 \equiv (p-1)! \equiv \left(\tfrac{p-1}{2} \text{ pairs } b,c \text{ multiplied}\right)$$
$$\equiv a^{(p-1)/2} \pmod{p}.$$

$$-1 = \left(\frac{a}{p}\right)$$

— If $a \equiv b^2 \pmod{p}$, then

$$-\left(\frac{a}{p}\right) = -1 \equiv (p-1)! \equiv (b)(-b)\left(\tfrac{p-3}{2} \text{ pairs}\right)$$
$$\equiv -a \cdot a^{(p-3)/2} \equiv -a^{(p-1)/2} \pmod{p}.$$ //

Observation: Since each quadratic residue has exactly 2 square roots, there are exactly $\frac{p-1}{2}$ quadratic residues and hence $\frac{p-1}{2}$ quadratic nonresidues.

Special case of Theorem: $a=-1$.

By ~~the~~ Theorem, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p$.

$$= \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Since both sides are ± 1, in fact

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Example: $x^2 \equiv -1 \pmod{107}$ has no solutions, but $x^2 \equiv -1 \pmod{109}$ has 2 solutions.

Fun trick: Suppose $p \equiv 1 \pmod 4$.

Then

$$-1 \equiv (p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)$$

$$\equiv 1 \cdot 2 \cdots \frac{p-1}{2}\left(-\frac{p-1}{2}\right) \cdots (-2)(-1)$$

$$= \left(\frac{p-1}{2}\right)! \cdot (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)!$$

$$= \left(\frac{p-1}{2}\right)!^{\,2} \cdot 1 \pmod p$$

Thus $\left(\frac{p-1}{2}\right)!$ is a square root of -1.

Example (playing a similar example):

$p=23$, so $\frac{p-1}{2} = 11$.

$$2^{11}\, \underline{11!} = 2^{11}(1 \cdot 2 \cdots 11) = (2 \cdot 4 \cdot 6 \cdots 22)$$

$$\equiv 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot (-11)(-9)(-7)(-5)(-3)(-1)$$

$$= \underline{11!}\,(-1)^6 \pmod{23}; \text{ so}$$

$2^{11} \equiv (-1)^6 = 1 \pmod{23}$. But by Theorem

$2^{11} = 2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod{23}$. So

$\left(\frac{2}{p}\right) = 1$. as it happens: (solutions are $\pm 5 \pmod{23}$)

Theorem: $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \quad (\pm 1), \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \quad (\pm 3). \end{cases}$

Formula: $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Proof: Let $\alpha = \frac{p-1}{2}$. Using the same argument as in the previous example,

$$\left(\frac{2}{p}\right)\alpha! \equiv 2^\alpha \alpha! = 2\cdot 4\cdot 6 \cdots (2\alpha)$$
$$\equiv \alpha!(-1)^r \pmod p, \text{ where}$$

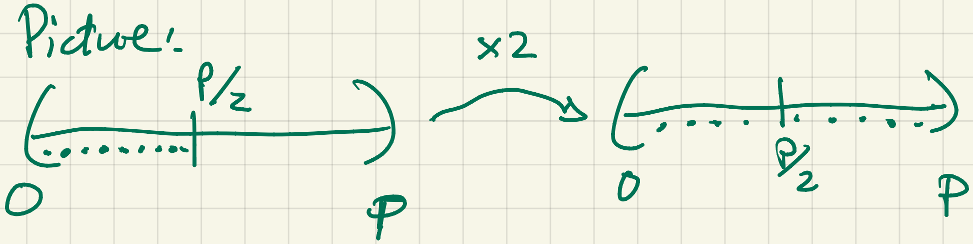
$r = \#\{1 \le j \le \alpha : 2j > \frac{p}{2}\}$.

Then check cases: $r = \begin{cases} (p-1)/4, & \text{if } p \equiv 1 \pmod 4, \\ (p+1)/4, & \text{if } p \equiv 3 \pmod 4 \end{cases}$

and check the theorem in each case.

Cancelling the $\alpha!$ gives $\left(\frac{2}{p}\right) = (-1)^r$. //

Picture:



and then count how many ended up in the right half.

Similar arguments can show that $\left(\frac{a}{p}\right)$ depends only on $p \pmod{4|a|}$.

But there's a master relationship that does all at once:

Quadratic Reciprocity Theorem:

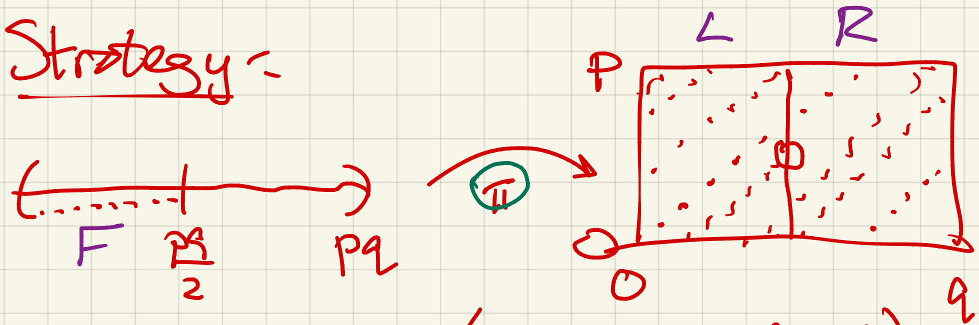
If p and q are odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

So $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ when either p or q is $1 \pmod 4$;

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ when both $p \equiv q \equiv 3 \pmod 4$.

Strategy:



$$\pi(a \pmod{pq}) = (a \pmod p,\ a \pmod q)$$

Count how many dots end up in R.

Notation: • $\alpha = \frac{p-1}{2}$ and $\beta = \frac{q-1}{2}$

• $F = \{1 \le k < \frac{pq}{2} : (k, pq) = 1\} \pmod{pq}$

• $L = \underset{(\mathrm{mod}\ p)}{\{1 \le a \le p-1\}} \times \underset{(\mathrm{mod}\ q)}{\{1 \le b < \frac{q}{2}\}}$

For any $\pi(k) = (k \pmod p, k \pmod q)$, either $(k,k) = L$, or $(k,k) \in R$ and then $(-k,-k) \in L$.

Check: The $(k,k) \in L$ and the $(-k,-k) \in L$ perfectly fill L. Therefore:

$$\prod_{(a,b)\in L} (a,b) \equiv \prod_{k\in F} \underbrace{(k,k)}_{\pi(k)} \cdot (-1)^r, \quad (\mathrm{mod}\ p, \mathrm{mod}\ q)$$

where $r = \#\{k \in F : (k,k) \in R\}$.

That is,

① $$\prod_{(a,b)\in L} a \equiv (-1)^r \prod_{k\in F} k \pmod p$$

② $$\prod_{(a,b)\in L} b \equiv (-1)^r \prod_{k\in F} k \pmod q.$$

Claims: we will show

• LHS of ① $\equiv (-1)^\beta \pmod p$

• LHS of ② $\equiv (-1)^{\alpha\beta}(-1)^\alpha \pmod q$

• RHS of ① $\equiv (-1)^r(-1)^\beta\left(\frac{q}{p}\right) \pmod p$

• RHS of ② $\equiv (-1)^r(-1)^\alpha\left(\frac{p}{q}\right) \pmod q$.

Assuming the claims: ① becomes

$$\cancel{(-1)^\beta} = (-1)^r \cancel{(-1)^\beta}\left(\frac{q}{p}\right) \Rightarrow \underline{(-1)^r = \left(\frac{q}{p}\right)}.$$

Then ② becomes

$$(-1)^{\alpha\beta}\cancel{(-1)^\alpha} = (-1)^r\cancel{(-1)^\alpha}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right).$$

ooo...

Claims: we will show

- LHS of (1) $\equiv (-1)^{\beta} \pmod p$ ✓
- LHS of (2) $\equiv (-1)^{\alpha\beta}(-1)^{\alpha} \pmod q$ ✓
- RHS of (1) $\equiv (-1)^{r}(-1)^{\beta}\left(\frac{q}{p}\right) \pmod p$
- RHS of (2) $\equiv (-1)^{r}(-1)^{\alpha}\left(\frac{p}{q}\right) \pmod q$.

(1) $\displaystyle\prod_{(a,b)\in L} a \equiv (-1)^{r} \prod_{k\in F} k \pmod p$

(2) $\displaystyle\prod_{(a,b)\in L} b \equiv (-1)^{r} \prod_{k\in F} k \pmod q$.

$L = \{1 \le a \le p-1\} \times \{1 \le b \le \underbrace{\tfrac{q-1}{2}}_{=\beta}\}$.

So LHS of (1) $= \left(\displaystyle\prod_{a=1}^{p-1} a\right)^{\beta}$

$= ((p-1)!)^{\beta} \equiv (-1)^{\beta}$

by Wilson's theorem.

Useful hack:

$$-1 \equiv (q-1)! = \prod_{k=1}^{\beta} k \cdot \prod_{k=\beta+1}^{q-1} k$$

$$\equiv \beta! \cdot \prod_{k=\beta+1}^{q-1}((q-k)(-1))$$

$$\equiv \beta! \quad \beta! \quad (-1)^{\beta} \pmod q;$$

so $(\beta!)^2 \equiv (-1)^{\beta+1} \pmod q$.

- LHS of (2): $\equiv \left(\displaystyle\prod_{b=1}^{\beta} b\right)^{p-1}$

$= (\beta!)^{p-1} = \left((\beta!)^2\right)^{\alpha}$

$\equiv \left((-1)^{\beta+1}\right)^{\alpha} = (-1)^{\alpha\beta}(-1)^{\alpha} \pmod q$.

We'll do RHSs of (1) and (2) on Tuesday; slight complication because

$F = \{1 \le k < \frac{pq}{2} : \underline{(k,pq)=1}\}$.